June 10-11, 2023

Washington D.C., USA

NORTH AMERICAN SCHOOL OF INTERNET GOVERNANCE

ACCESSIBILITY AND INCLUSION

2023 North American School of Internet Governance (NASIG)

June 10-11 2023 – American University

(raw transcript)

11 American University Research Space

>> Derrick: Thank you very much. Emily and I really excited to be here today and (Away from microphone).

In research entity that can facilitate research in the Internet governance space. I am Derrick Cogburn.

As you know you've seen me over the last few days. As I mentioned earlier, you only have one more time to see me and that's in the summary. Emily you want to briefly introduce yourself.

>> Yes, thank you very much Derrick. And first of all can I say thank you so much for hosting us here and being such a wonderful research partner for us at the DNS research federation. We really appreciate the collaboration. My name is Emily Tailor. I'm the CEO of Oxford information labs and over the last year or 18 months we have been setting up a new nonprofit called the DNS research federation and it's dedicated to raising awareness of the domain name system and the intersection between the Internet's architecture and

the sort of contemporary policy issue, cyber security and technical standards. So we do that through research and so on. I'm actually doing our intro but I'm also an associate fellow at chat ham house and editor of their journal of cyber policy. So thank you.

>> Derrick: Excellent.

So the structure of this panel you see while you were away at lunch we reinstructured the panel this. Is the mega panel for the day. So -- yes, we're very pleased for everybody that's here. So let's give them a big round of applause.

[APPLAUSE]

>> And what we will do is firsts have a presentation on the DNSRF and overview of the data analytics platform. That will be Emily's colleagues Mark and Georgia. Thank you.

>> Emily: And then we'll go into several of the research projects that we are supporting and we'll start off with you Derrick and your colleague Andrew and is Heman coming as well.

>> Virtually. She's already in.

>> Emily: Fantastic.

And then we will have a presentation on ransomware project from Divia and Erin and that will be delivered by video. And then we will come back to our own Mark Datysgeld here who's an independent researcher from Brazil and also a member of the GNS account so at ICANN.

And then we'll be doing Q&A.

>> Derrick: Q&A.

>> Emily: We're hoping that we will have a good solid interactive session with your questions. We've got enough to talk about among ourselves. So don't worry if you don't have questions but we want to come out to you as soon as we have got the talking bits overwith and get to your questions. So we're really looking forward to that.

>> Derrick: Absolutely. I'm going to say this once and I'm sure you'll hear it two or three times. After this is over, there's a reception outside and an opportunity to view the data analytics platform in realtime in Room 603. So that's the first of two or three times that we hope you can hear that because we would like to you come during the reception and the

break and to take a look at the platform and maybe ask some questions, do some queries, things like that.

All right?

Shall we get started?

So this collaboration is something that we're really excited about. American university was asked by the Oxford information labs to be a partner in DNS research federation. And in preparation for the launch, the DNS federation reached out to Universites and university researchers to think about projects that could kind of form the initial basis of our collaboration. And so do you want to say a little bit about the federation?

>> Emily: Yes. The DNS research federation is a nonprofit. We set it up about 18 months ago. We're very fortune to be seed funded by meta and also been gaining research funding from bodies like the Internet society foundation, Arin and also ripen CC and others as well.

So as I was saying earlier, our mission is really to try to connect back, if you like, to the sphwernt's architecture and we were really talking about that in that excellent I first panel, formats such a strategic function and yet hardly anybody knows about it. I was really struck by what Wolfgang said that John Pastel was like if you dress everything up with acronyms then no one knows what you're doing and everyone leaves you alone. Well, we were just doing some consumer research on that a couple of months ago and we added some domain name type ones into there and we found more than 70 percent in the US don't know what the DNS is. Significant minority thought it stood for the deaf and nude diss society and when asked what a domain name is only 36 percent really could answer that accurately. And when you think probably those same people could have a good go at AI, block chain and a lot of the other, you know, technologies that have come later and are probably not involved in absolutely every interaction that the people do online. So we felt like this was a gap that needed to be filled. So we achieve our mission through education and research, access to data and I'll give another plug for the live demo and also involvement in standards and Carolina is our standards lead so please do catch up with Carolina in the break if you haven't already.

So this year, we have been doing a lot of events, and also what we'll be hearing from you and the other researchers about today are components of a special issue, the peer-review journal, the journal of cyber review policy from Chatham how's. That I hope will be published by the end of the year, fingers crossed. We've got some events this week. Very busy at ICANN doing a round table on block chain domains which is some research that

George and Nathan have been doing and also here we are at our -- the NASIG event together. Georgia is going to talk to you about the community of researchers but also in our Web site we have an online research center which is going to be the home for all of the projects that we have been doing. You can already see RPKI project, Internet standards observatory and as we start to complete the research projects that we're doing either through the DNS Research Federation itself or through independent researchers like yourself and Mark and others, they will be there in that research center. So that will be a resource for everyone.

But mainly and I was really, really inspired by the previous panel the speaker is talking about how they're building communities and that's really going to be what we're doing as well.

So I will leave it there. I talked enough and then go back to my moderator hat. So thank you for that opportunity, Derrick.

>> Derrick: Thank you. Absolutely. We're looking forward to building community with you. So thank you for being here. We're really excited this could come together. So thank you. Please join me in welcoming our colleagues.

[APPLAUSE]

>> Mark and Georgia.

>> Mark: Welcome. My name's Mark and I'm the CTO of the research federation, one of the founding directors as well. Really great to be with you. I must reiterate my thanks to Derrick in particular to inviting us to come and join you today. And it's been a real pleasure to work with you over the last 18 months. Been a real sense of collaboration and clegiateness with you. So thank you first of all before we start. So I'm going to talk first of all about the DAP platform, DNS analytics platform. This really is fulfilling the second point that Emily made in her bit a minute ago about providing access to data and our commitment as the federation is try and provide as much data access as possible in sort of unbiased way to let the data speak for itself is kind of our mantra with the platform. The DAP is our means of providing access to data. We'll talk a bit about how that structure the kind of data we have in the platform going to the next slide.

I think just to set the scene where as an organization very committed to sort of open standards working open way. So all of our software is built on our sort of open source components using open standards. We have a sort of 20 year history as a company in other guises working in software architecture and particularly in systems within the DNS

and Internet space. So we come to the party prepared with lots of preexisting material. So whilst we have been going for approximately sort of two years now, we have the software foundation for this project has been built on lots of years of try and tested software. That sort of sets the scene for the platform.

So we like to see that the platform as being in three sections. Input is sort of data coming into the platform, analytic which is is working with data and analyzing data to provide derivations of data and other sort of computational aspects of data and finally outputs which is the way in which we sort of get data back out. Our system's very much a two-way system where data comes in, is manipulated and then data goes back out again. So we start by looking at the input side of things. We have a number of existing foods that we provide. I think we're slightly unusual in that we haven't gone to the market looking for particular data. We have been driven a lot more by other key sort of idea which is to be really -- being driven by research. So looking at research problems rather than just going out and looking at data for the sake of it. So we have quite a wide range of data at the moment. Sixty plus feeds at the moment on the system ranging from some of the more classic data you might expect to be looking at such abuse data, fishing malware scam data that kind of thing but also looking at other data to do with ranks CSO contributeing fact to looking at how sort of systems are represented on the Internet and also how well sort of sites are performing as well. So that's really important to us too.

Also, coming back to the research point, we've recently done work in looking at block chain domains in quite detail so we've got data on that which is again not a more usual sort of study sets and also other types of data around the structure of the Internet. And it's an ever growing set of data, we're very interested in people's problems and what people are interested in researching. Always looking for new ideas for data we can bring on to the system. That's very much our approach.

The final thing to mention as input is that we have an ability to bring your own data and that's something we see is very valuable. Often people like to start with their own datasets, enrich it with some data that we provide in the platform and then get the data back out in a format that's used visualize the data. Bring in your own data in a secure manner in a way that's protected to only your space, really important feature of offering that's part of the DAP system. So moving on the to the analytic side of things, we aim to provide a fairly straight forward we like to call it sort of an Excel plus experience. We're not looking here at people who necessarily -- people very technical or people who can write database queries. We're looking at people who can operate Excel to a relatively high level who can maybe write formulas and that kind of thing. Provide the sort of tools for joining data to other sets within a system, especially for summarizing data, creating your own formulas, that kind of

thing. The kinds of things you expect from the analytical system in that sort of way. Again mentioning the fact we allow you to bring your own data, being a very key part of that as well.

And of course a final section to talk is output of the system. We have a number of different ways you can work with the data and sort of get the data back from the system. Office ones are visualizations which we have available in the system. Also have the ability to export data using custom API connections back to the system. And you're free as a user to create your own APIs within our own environment to really have quite fine grain over getting data back out in formats suit your needs in different ways as well and we mentioned before you have very control about a very important to security is very important to us as an organization and most of the data system is locked to your project only in the system therefore there's no sense anything you do will be available to other users if you choose to share in that way.

Another thing to mention briefly is alerts. One of the user systems in and then cases looking at changes to data over time and many of our users like to be able to track data and see what's happened over say daily or weekly or monthly cycle and to be able to receive automated alerts via e-mail or other forms to get alerts on when data changes specifically. So give you sort of some quick slides about the output side of things here, here's typical dashboard would he have created in our system. This is looking at block chains as an example here but you can see a rich set of presentational tools much like other dashboards you got charts and graphs and tables and other types of presentations there.

Another thing that -- Emily alluded to is that we've created the research zone with the DSNRF Web site and that's another very important way in which we share data back to other systems. So for ourself, we have created a research zone here and this is to do with a project we're doing to do with standards tracking, but you can see on the right-hand side here that we've actually got a latest activity chart that's being fed from the -- with itself with the standards and example of more advanced use of our system for tracking documents which is another feature that we support and you can see we've actually got direct integration with our own Web site and adapt system to achieve that in a very rational way.

I think that probably completes my section but it's been really great to speak to you all today.

Thank you. Here's Georgia.

[APPLAUSE]

>> Georgia: Good afternoon, everyone. My name is Georgia Osborne, senior research analyst at Oxford information labs but also the research community manager for DNS Research Federation. So you will hear some of the research community today speak about some of the projects that they have done over the last year. We are data led, which means that we are evidence based and we are kind of neutral in that. We follow the data. My background is not intack. It's an as an intelligence analyst. That's what I really care about. The research from reports that we produce are sort of something that we share around. I think it's really important that the research community helps to bring data to the research and make it so that it's a conversation. So we're bringing data to the researchers and building research and reports but also building this community where they can meet bilaterally, they can meet in multistakeholder environments and forums like this, discuss big research projects and really influence policy. So this is sort of what we're trying to build here as part of the research community. We're going to be in Room 603 I believe with some of our dot data but also just to kind of talk about things. As Emily said in the beginning, I did a research project as well. So also doing research in block chain domain names. I can also answer any questions about that later on. But without anymore delay, I'd like to go back to Derrick to talk about some of his research. Thank you.

[APPLAUSE]

>> Derrick: Excellent.

I'm going to ask Andrew to come on up and we have Haiman online. If you could turn on your video as well. There she is. All right.

Well, we are really excited to share with you some of the first look at some of the work that we have been doing and we chained the title on you a little bit (Away from microphone) exploring 23 years of ICANN's uniform domain name dispute resolution policy through computational text mining with implications for private ordering.

[LAUGHTER]

>> Some of you know I like to have dissertation titles for everything that I do, but this was really exciting problem for us. So some of you yesterday might have heard me talk about kind of my own research trajectory going back to 1998 working in the Internet governance space very very early on and lots of problems that we wrestle with over the years and it ended up with a discussion that was out on researching Internet governance. The chapter that I wrote in that book really focused on how computational text mining could contribute to Internet governance research and what we did in that chapter is we looked at all of the transcripts from Internet Governance Forum going back to the beginning of the Internet

Governance Forum. And we answered all kinds of questions about what IGF has focused on, what has been his themes, what are some of the core issues, what hasn't been addressed? It was really a fantastic chapter. For those of you who bought the book yesterday, thank you. And for those of you who haven't yet,.

[LAUGHTER]

>> (Away from microphone).

>> Derrick: Only two types of people, right?

[LAUGHTER]

>> Derrick: I will say the book is open access thanks to a generous grant so the book is open access but I do appreciate you buying it. So out of that chapter we start thinking about well what could we do in this interesting collaboration with the DNSRF?

>> The book is available as a resource already in the Web site of NASIG 2023.

>> Derrick: Fantastic. So you just deprived me of all of those possible sales.

[LAUGHTER]

>> Derrick: I'm just jokeing. I'm just jokeing. Thank you. Know your friends, you know? No.

So we started to think about what could we do with that same technique with this collaboration that could ab lot of fun. So we want to talk today a little bit about kind of this process? We'll talk about this problem that we're trying to address, some of the literature and conceptual framework, some of the questions that we're asking, our methodology, findings and some discussions and we're doing all that in 15 minutes. So a lot to cover. First off, we had a little tutorial today for those of you who are new to this space talking about domain names and IP addresses and why domain names are so important. We know that more than 351 million domain name registrations and they increase about 10.4 million annually. These are multiplying very quickly. There can only be one unique domain name per top level domain. So these are unique resources and they engender a lot of competition. So some of this competition is known as the trademark dilemma. This is domain names that are engeneraldering competition because somebody owns them, registers them, registers a domain that somebody else in a trademark that somebody else already owns or you find domain names that are just generic names like an apple, I had an apple for lunch, right? And a trademark holder like apple computing will say that's our

mark. So you have some legitimate and some illegitimate sources of competition. So sometimes it's just and then you have this whole series of the Apple sucks, obviously I don't think so. That's free speech. Where should that become a problem? So this kind of competition really was a problem from the beginning of ICANN and wrestling with how do you deal with this global trademark dilemma problem? And so in 1999, ICANN adopted the UDRP. It went into fully functional in 2000. So lCANN mandates that it's users -- its registrars required the registrants to go through this domain name dispute resolution process. So if you have a conflict which you're going to see there are many many of these conflicts, that's where you start. And the reason for creating this process was to try to handle these legitimate and ill legitimate competitions over domain names themselves. And so they appointed six dispute resolution providers. We call them DSRPs and there are six of them: There were previously two others and you can choose which of the DSP -- DSRPs you go to. The UDRP process requires a person who's making the complaint. They're called the complainant. That's tough for me to say. The complainant brings the case and they can choose which of the DSRPs they file with. So one of the things that that led to was the possibility of forum shopping. Are there differences between the DSRPs such that if I have a certain kind of case I take it to 1DSRP. And if I have another kind of case I take it to another DSRP. And so the panel can either be an individual -- heard by an individual panelist or a panel of three panelists. And there's a three prong test that's in the policy. Is it -- is the domain name idol or confusingly similar to a trademark or a service mark so that's the first part of the test. That the person who registered it has no rights or legitimate interests to that domain. And it's registered in bad faith that the complainant has registered this and it's being used in bad faith. So if -- just as a hypothetical, if you registered Apple and you were selling apples, then that has -- that's a dispute that is going to go through this process because it's not in bad faith. But if you registered apple and you're talking about computers and you're selling computers that are gray and silver and look like they might come from Apple computing, then the panel is going to look at that slightly differently.

So over the years some people have lawedded this process and some people have challenged this process. Their whole range of challenges to look at this. And we want to talk just a little bit about some of the literature around this. So Haiman, do you want to say a little bit about the literature and just tell me next slide.

>> Haiman: Our literature review you can go ahead and jump to the next slide here really started with one of the core tasks that was assigned to ICANN upon its initial establishment and one of those initial tasks was the trademark dilemma which Derrick talked on briefly before. And what it refers to is the challenge of register domain names to those that first

claim them while respecting trademark law. So as Derrick kind of touched on before the trademark dilemma began with the realization about kind of the market with commercialization implications that could occur if the trademark dilemma went unaddressed or there wasn't any intervention to really address that. So to address this trademark dilemma, ICANN collaborated with WIPO and yielded this report where they recommend both the three stage three prong task that Derrick just discussed and also recommend the establishment of a mannedstry administrative procedure concerning abuse of registrations which would allow for a neutral venue in the context of disputes that are often international in nature. So that kind of gets into the UDRP process that we have been talking about. The UDRP process a lot of the literature and a lot of the law review us that have kind of analyzed the merits of it have lawedded the process for the strides that the process has made in showing how it's possible for an international nonprofit and privatized entity such as ICANN to facilitate dispute processes over domain names in a way that encourages participation from countries around the world in a manner that's oriented towards multistakeholderrism when we talk about Internet governance. Despite some of those strengths critics have talked about the process can suffer from inconsistencies and biases in favor of trademark owners, kind of the threat of the forum shopping or venue shopping that Derrick touched on before and also the lack of an appellate body and potentially affording panelists too much freedom. The next slide talks about how we can address some of these limitations. So previous studies have recommend everything from distinguishing the process as a new independent process that shouldn't be equal to arbitration. They've talked about ways to kind of expand the UDRP process by including country code solutions or even, you know, other types of trade names within the trademark process. They've also talked about, you know, remedying the UDIP process so that ICANN chooses the provider and creates a UDRP oversight board to eliminate some of the biases that might occur. And one of the last recommendations is that the UDRP should provide clear legal guidelines and consider limiting the publication of UDRP decisions by each forum to prevent that issue of venue shopping by the complainant. There's a lot of different suggestions, work around what can be done to improve and strength then the UDRP process. A lot of good praises about it too. So the -- on the previous slide we talked briefly about the conceptual framework that's right here. So we start with all of the UDRP disputes and we get into the complainants and respondents and then we break it down into the four main DRSPs that are included in the study. I'll turn it over to my colleague Andrew to go over more of the research questions and our specific methodology.

But thank you.

>> Can I just interrupt a minute to for giving credit to our captioner for keeping up with that. Her name is Emily. Thanks Emily.

>> Derrick: Thank you Emily. Yes, thank you.

A different Emily.

When we started this process and first made our proposal to the DNSRF, we had identified the UDRP decisions as our source of data. It's what we thought we wanted to mine. We knew that there were studies that had looked at venue shopping small chunks of the decisions and we thought with a computational text mining approach we could look at all of them. So when we made the proposal there was this nice third-party site that was making all of the complaints available and we said oh we can use that. We'll download that data and use it. And by the time on the addition of the proposal that was gone. So we said oh shoot.

That wasn't exactly what we said.

[LAUGHTER]

>> Then we said well we can scrape it. Andrew and I and the team we said we'll scrape it ourselves. We can scrape it. We started writing that and it was taking a lot of time to do that and we had our conversation with the phenomenal Mark. Mark said, oh, we can do that.

[LAUGHTER]

>> We can do that for you. So we had a good conversation about what we would like, what kind of data would we like so they've talked about how they want to be data driven and researcher driven and so we said we'd like all the complaints from all of the -- we'd like these kinds of variables which is what we would like to capture if we were downloading and scraping ourselves. So as you will see these happen very frequently so they also agreed they would update this and keep it up to date. We said Bravo, we're delighted that's now one of the datasets available on the DAP live platform.

Andrew, why don't I turn it over to you.

>> Andrew: All right. Yeah, so at the first start, we started with 75,590UDRP cases. That's how many we found on the DNRSF's Web site. So here what you can see is the average number of cases filed over the years. The average number was about 3,055. The peak was in 2022 with 7100 and that was a 27 percent year-over-year increase on the previous peak

in 2021. And as of June 2023, to Derrick's point, the DNRSF keeps updating the data. These are the cases that have been filed as of June 2023 and if that rate extrapolates we expect around 6,000 cases by the end.

The next thing we looked at was the number of the main names contested per case. So 83 percent of the UDRP cases had one domain name contested and over 90 percent had three or fewer domain names. What that means is most of these disputes are not these big coordinated efforts and stuff. But the number of large cases, however, and large was arbitrarily defined as above six. We took that from previous research. So that increased 1.4 percentage points compared to that previous research. But on an absolute basis there were over 100X increase to about 2,577 cases. So now you start to see the sophistication kind of coming in. And then 245 or more which the previous research didn't have, there are about 12 such cases and we called those extra large caches. The largest case we had in the dataset involved 1,529 domain names. And that respondent actually has a total of over 20,000 domain names. And they -- yeah, they use that for illegal purposes.

So the next thing was to look at the marketshare between the DRSPs over time. WIPO is dominant overall with 55 percent followed by NAF. And then dominant marketshare between 2000, 2022, we see WIPO dominated 18 of the 22 fully reported years compared to NAF, which was five of the 22 years.

So the next thing we looked at was outcomes. And so trademark owners are big, big winners. So 90.9 percent of the cases are either a result in a complainant winning or complainant terminating or settling the case. That has increased 10.9 percentage increase to the paper we found in 2001 and then respondents only win 8.9 percent of the time. And then .2 percent of the time the results are split decision. We also tried to break out some nuance by looking at these outcomes by DRSP and the outcome ratios for winners are about the same, except NAF had a bit fewer and the ADNDRC was a bit higher and stuff.

Next.

Decision time. So the number of days to make a decision has been found as a critical variable in whether case is brought to DRSP and to Derrick's point, these complainants basically can vanish up. And of the 2DRSPs that were closed were actually closed because they weren't getting enough cases basically. And so just a few caveats here. So this was only for CAC and WIPO. For WIPO we filtered decision times between 28 to 365 days because that's the data that seemed to be most accurate from the script. And so we can see there are differences between the DRSPs. On average, across everyone it took about 63 days to file a complaint and then the other thing we did was we just made a binary

variable. How many cases decided six days or more, 60 days and less and we can see that for WIPO53.5 percent of those cases we decided in less than 60 days.

The next thing was to try to look at decision time based on the results. And so the really interesting finding here was that complainants, their cases were decided in less than 60 days about 55 percent of the time compared to only 37 percent for the respondents. So if you're a respondent, good news, the longer it takes the more likely you are to win, but you're going to still have to wait a while. And so this was just looking at the average time for cases or over time and we see a shift. So between 2000 to 2008, 45 percent of cases were decided in less than 60 days compared to from 2009 to 2022, 58 percent were decided in less than 60 days. So our two possible reasons for that is just the maturity of the UDRP and then again our dataset heavily leans WIPO. So WIPO has the dominance. They get the precedent. They understand how to be more efficient and then they use that to keep building their lead.

The next thing we looked at was was the most frequently occurring words in the dataset so we added a custom stopper dictionary to filter out some unnecessary words. And so a few interesting words we see are patent. So panelists always seek ago patent of certain behavior from respondents. The next were Google farm and insurance. Farm and actually State Farm Insurance and those refer to regular cited precedent cases. The UDRP as you look at it now is built on precedent and they use a lot of precedent in making the decisions. And then we also find typo squatting which is a quote/unquote cyber crime if you will.

Then the next --

>> Derrick: People register domains almost like something else hoping that you make a typo then you get sent to their site rather than the trademark holder's site.

>> Usually used to demonstrate bad faith.

The next thing was the most important occurring words we used term frequency and verse document frequency to kind of figure this out. And these are just the top 25. As you can see a lot of them are trademark holders, which is not a surprise. And a bunch of those trademark owners, what that involved was some of it were their own cases and others were cases where they've now become president and are being used as such. I will turn it back to professor Cogburn.

>> Derrick: Thank you so much, Andrew.

So when we look at sort of what this means for us, is early on people thought maybe this process would become irrelevant, that it would start to slow down, people wouldn't keep

registering these domains and the competition might decrease. And we see from this data that it's far from slowing down; it's increasing and the most -- the highest number of cases occurred in 2022. 7,000 -- 7100 cases in 2022. Again, most URDP cases involve only one domain name. So not these big mega cases that you might hear about sometimes. That WIPO plays this dominant role followed by NAF. Even though you have four other DSRPS that are out there.

As Andrew said, the complainant wins the vast majority of complaints brought to the UDRP process. So this idea of is this -- if you go back to earlier when we talked about why is this established, to try to have a relatively fast, relatively inexpensive process to mediate this trademark dilemma, this competition. And so.

If you think that the person who's been wronged, the complainant, is bringing the case and they're winning, the vast majority of the time. So that suggests that this process is working.

The decision time, a low of 36 and a high of 63 does say there are differences between these DRSPs. We have more work to do to tease out some of what the substantive differences are between these DSRPs -- DRSPs, we have been talking about what do we call these things? And so the acronym's tough. So there are differences but we want to tease that out.

So this concept of private ordering. So here you have a nongovernmental entity, a global nongovernmental entity, not a legal process that can intervene in this competitive space and take a resource from somebody that owns it. And that's a pretty significant role to play for a nongovernmental entity to be able to take something like that from you. And lastly we'll just say that the text mining approach we believe is very, very valuable. We think this study is starting to show that. But we also believe this is only scratching the surface. There's so much more that we can do and that we will do, some of which we'll do before next week.

[LAUGHTER]

>> And, you know, we look forward to having a conversation with you about this work.

I want to thank Andrew and thank Haiman for all of the hard work. So thank you guys.

[APPLAUSE]

>> Moderator: Derrick and Haiman and Ann Drew drew, I know we're going to come on to Mark and we've got the video from Divya and Aaron but that was a rich presentation.

Thank you very much indeed. I wondered if there's any immediate questions or reactions. Yeah, I thought there might be.

[LAUGHTER]

>> So why don't we just take those before moving on because it's a really substantive piece and while people have got it in their mind.

So I've got a gentleman at the back there, lady in the middle and then Jonathan you wanted to come in as well.

>> Who's first? Do you know who you are?

>> My name is Raymond from Ghana. I want to find out one do you have any idea why WIPO is the preferred entity and what are the cost comparison among the entities that handle the resolutions?

>> Moderator: Let's just take the request he is and come back to you.

That's from Raymond. Why is WIPO preferred and what are the costs (Away from microphone).

Sorry, so from Raymond from Ghana we've got the question on WI -- why is WIPO the preferred one and also any cost differentials between the providers. Maybe we can take your question and then Jonathan, so it's a lady here in the red. And then you've got one at the front here and I think one -- oh, gosh. Oh my goodness. Right. Let's take three and then we'll come back for another three and then we'll come on to the rest of the presentation. So thank you.

>> Hello. So my question is, as you mentioned, DNS research foundation, so how you are -- what are your plans to involve the larger research community into DNS Research Federation and I mean what is the process to get involved with any of the research projects that might be running under this initiative?

>> Moderator: Thank you very much.

Jonathan, did you --

>> Jonathan: Sure. My question was I saw earlier in the slides that there was some finding of -- by some researchers in terms of bias toward trademark holders and the data shows that they win most of the time but it's very difficult for me to tell how you would tell from the type of research what the quality of an outcome is and therefore is it just an indicator

that the right people are making complaints for the right reasons or is there in fact a bias? I would be very interested in how you're trying to address that.

>> Moderator: Thank you very interesting. So I've got three here. The one on why WIPO is preferred and cost. There's one on the DNS Research Federation which I can take, but let's hear from you first on the quality of outcome and bias. And I was also wondering actually to Jonathan's point whether you're looking at the response -- whether a respondent has responded and whether that has an impact on the outcome of the case.

>> Derrick: Right. Absolutely. Great questions all around. First in terms of WIPO. As we tried to show very early on WIPO was involved with ICANN to set up this process. So it has a great degree of credibility in this process. Another aspect to it is WIPO is focused on intellectual property. So it's seen as an international venue that is designed to be as much of an honest broker as you might be able to find in a global arena. The national arbitration forum is also popular because it's based in the United States and it has this sense that US or sometimes western trademark holders would go to the N AF as a potential venue. The cost is an issue. It's certainly there are differences in costs between the DRSPs. That's why they called it RSPs before. DRSPs.

There are cost differences. We'd have to go back and look at our notes just to compare the cost. That's another key variable. One of the things we found is there's so many interesting variables for us to tease out we just have to choose which ones we want to use but that is an issue.

And in just -- I'll deal with Jonathan's question. So in terms of bias, we have so much to draw from in terms of each specific case. So we have some strategies around using some machine learning strategies and so forth to try to understand what does a successful case look like and what does an unsuccessful case look like to see if there's more than just time to decision for another reasons of why you might choose 1DRSP over another one. So there's a lot more than we can tease out from that process.

Andrew, anything you want to add.

>> Yeah, just to touch back on the costs, most of them are about 15 howntdz low end. I do know NAF tends to charge more based on the number of domains you're filing for, same as WIPO but up to five you get around 1500. So the cost differences aren't really too big enough to explain the difference of why WIPO is so dominant.

>> Moderator: Have you looked at the response rates as well and whether -- you know because my impression is most of the cases are uncontested. Is that something that's popping up on your analysis yet?

>> Andrew: I'm going to tease that out because you guys did scrape the response contentions part. There is a bunch of rejects, right? I'm sure as Mark and his team know, processing this data was not fun.

[LAUGHTER]

>> Yes, so we have to come up with that to figure out the actual people who didn't respond and we will include that as part of our final journal of cyber policy.

>> Moderator: Great, thank you.

>> Derrick: And it's really interesting and that's why Haiman if you want to jump in one quick second, the literature is pretty rich out there of people that have looked at some of these questions and the question of costs, you know, certainly came up before, and this sense that a person that doesn't have a legitimate -- and there's a a little bit of a debate here and tough to tease this out that a person who doesn't respond either -- so there's a sense a person who doesn't respond is doing something elicit so they're not going to respond, not worth their time but there's another concern that if a person is a small organization, doesn't have a team that can write the response, doesn't have enough time to be able to respond, then they don't respond and they're sort of treated as if -- don't have enough money, exactly (chuckles).

Then they're treated as if they're a bad actor in this space.

>> Moderator: I'm counting at least six more questions. To the lady about the DNS Research Federation, yes, we are very actively interested in engageing with the wider research community. Do keep an eye out for calls for papers and we're constantly -- we're partnering with other Universites as well looking for more and very much have an open door because we want people to be interested in this space and we want to help to stimulate that research that will bring it back into the main stream where it belongs in my opinion. So thank you.

>> Derrick: Just one quick comment there as well. My team, we look for researchers who might want to work with us as well, particularly who can bring skills to help us immediately. We don't mind bringing on people who need to learn a little bit more and be trained and so forth, but if you can hit the ground running and helping us, that would be even better and

we work very well distribute it, so much so that this is my first time meeting Andrew face-to-face. I've known him over a year.

[LAUGHTER]

>> Derrick: I met him at the same time as the rest of the team here. So we're happy to work with people remotely.

>> Moderator: Thank you very much and I know that I've got like loads of people wanting to ask questions. With your permission, hold those questions because I think we could talk out the rest of the session on this fascinating piece of research. And I want to give space to Divya and Eireann's video presentation and then have Mark, because I think once you've heard from Mark you'll want to ask loads of questions about what he's been doing as well. So I'm really pleased at the level of interest we're seeing in the room.

Joly, could you line up --

>> Derrick, do you want to stop share screen?

>> Derrick: Will do.

>> Joly: Just let me make sure I've got it on the live stream as well as this. Yes, okay.

Okay, I think we're good.

>> I'm going to pull a cannia west --

>> Good afternoon, all. It's really a pleasure to be able to present at least in this recorded format to all of you about my on-going research and of course now my collaborative research thanks to the DNS Research Federation. So a little bit about me. My name is Divya Ramji, doctoral candidate and soon to be defended doctoral candidate at American University. And would you like to introduce yourself?

>> Sure. Also all around awesome collaborator.

I'm Erin, CEo of consensus risks we gather big claim ran some aware data, also former academic Cambridge risk studies and DNS Research Federation who brought us together.

>> Divya: Today we're going to go over a little bit of my on-going research right now with my dissertation of how I'm trying to better understand ransomware and how it is becoming improved having a better model thanks to the data analysis from my wonderful collaborator.

>> I think the model was fine might I point out, just it needs some data. Any ways we'll talk about that.

>> Divya: Let me go ahead and share my screen, get some slides going.

So for my dissertation, I really was trying to understand this phenomena of ransomware attacks across the United States and how could we better measure and understand how entities are attacked and also how entities recover from ransomware attacks. So for me, I find it an interesting myth logical problem of how can we better measure this. So as a social scientist, of course, two major issues that we always have are how can we handle missing data and how do we handle measurement error? These are two issues very much so when it comes to understanding cyber crime. For me when I was trying to understand ransomware attacks, I really had to kind of whittle it down to understanding ransomware attacks gengs critical infrastructure entities for my project because there really isn't much open source data about ransomware attacks in any kind of cohesive form. So for the project, I actually was able to get a dataset because that is currently maintained by Temple University. They have a lab there that looks at prevalent infrastructure attacks. And so they provided me data from 2016 to present about ransomware attacks that had been specifically targeting critical infrastructure. When I say critical infrastructure, these are sectors such as, you know, government healthcare education that have been designated as critical to United States infrastructure by the Federal Government. So moving forward, how can I try to handle the idea of missing data and measurement issues when it comes to understanding ransomware. So my two approaches for that were to understand it looking perhaps at just a very strict time series approach. So really trying to look for what are the patterns over time. Is there a way that we could use what we have in terms of existing to predict how ransomware will evolve over time. We know that ransomware has very clearly increased but, you know, it doesn't necessarily increase any linear way. There are peaks and valleys along our time line. If I fit a model to thisda, could I actually use it to predict and understand how many people are being attacked over time as well as how many people are recovering over time. And then in comparison to that, I want to use a different type of approach considering how much dynamic features are when it comes to ransomware attacks, not only from the criminal perspective whether it was a gaining or individual or state sponsored but also from the victim sponsored of whether it's individual, local company, a major healthcare provider for the entire country, a pipeline company that is supplying gas for the entire country as well, or company like Microsoft that has global influence. So compound mental modeling allows for a little bit more flexibility when it comes to understanding how we can sort of thinking about ran ransomware within different types of clusters.

So, again, my time series approach, I try to use my -- the data that I already had which is again very limited. I fit a model and as you can see sort of on the right-hand side of this, it didn't really work out very well when it came to predicting what was to come based on the data that I had. And so very clearly right now the open source data that I was able to attain, the trends within it are way too unstable for me to be able to make accurate predictions and really understand what's going on. And there are different ways you can tweak this model as well just to give an example. I tried a different type of smoothing technique to see if that could help and I found a certain model that fit the data better but it's nonetheless that model still was not very good at predicting in the future how ransomware was going to evolve. Really kind of validates that yes I need to try a different approach. So that brings me to that compartmental modeling perspective. This model has been used quite frequently in various other fields. It has also been used itself within cyber security but only looking at things within a company itself. So a work within a company of how a company is attacked and how that attack then police officer rates within their network of computers and things like that. For me I was thinking okay if we're able to use that on that micro scale can we use it on a macro scale on the United States, its own scale. The critical infrastructure being all these targets that can be susceptible to attack. Here I'm wanting to use an SIR model. It's a very common model from epidemiology. Trying to understand how a virus spreads and one reason I wanted to also lead into a SIR model epidemiologists use this very much to tackle the issue of underreporting which as I mentioned is a big issue here. So here I've split my population of targets, which is critical infrastructure entities and SIR which are susceptible entities, people who are infected have succumb to ransomware attack and people recovered. Really my main interest here is understanding understanding how people are moving from one state. So going from susceptible to infected and also going from infected to recover. And those are those beta and gamma rates of change. And so a particular interest to me is gamma rate of change and understanding how an infected entity can go into recovery status. How are they paying ran some aware.? How quickly? Are they paying? And things like that. So when I actually run the model like this, I can get -- I get various types of outputs when I try to tweak those rates of change based on different types of information. And so in my work I realize really that rate of recovery change -- rate of change for recovery is the more important rate to try to tackle and gets me better model outputs. So for that, I really -- I needed more data in trying to understand how are people making these payments? How frequently are they making these payments. You know, who are the gangs that are targeting? Is there a way we should be clustering the space on maybe sector or even the gangs and the way they're targeting these victims. And so that now brings me to the -- my wonderful collaborator who will then extend upon that.

>> You've disabled -- oh.

>> Divya: Of course technical issues when talking about technology.

>> Eireann: All right. Want to just get the presentation up. There we go.

So I'll keep it brief because we want to not spend too much time but I've walked a mile in Divya's shoes as a young researcher. I couldn't get the data that I wanted to work on critical infrastructure stuff. Found it really frustrating. And getting good data, you know, makes a big difference. Some of the models that she's been using work. They just work on different dataset. So I have a very different dataset looking at 140 thread actors over about a decade. We have 120,000 bit coin addresses that we track for payments of those different groups. And we can see the amount of money paid, what time it was paid for those different groups. You can see on the left-hand side those different groups categorized on a log scale. So some peaky ransomwares in the last few years showing up.

One of the first questions we wanted to answer was are ransoms getting worse over time? We did an experience coefficient correlation between amount of time and the ran some and the short answer is yes. You can see here the p-value is very low. So in you have to reject the null hypothesis and say ransoms are getting worse over time. So the ones that we see are getting higher. Interestingly, the frequency has dropped. So there is less ran ransomware attacks or less paying of victims according to the data that I'm looking at but the ransoms they are paying are much higher. We published this paper in 2020 and in it we showed that power logs could be used to fit the data in ransoms and the alpha of those power logs suggest they don't have a while to find average for most of the years in the study. And so you really shouldn't use averages to characterize ransoms. Everyone's still does but we discourage that. We say you should really publish a median and a mode as well as the average if you're going to do such a thing. And the reason the averages don't really capture it's kind of like if you put Divya and I salary together and average it then it might say something about the two of and you say the amount of money we earn and our lifestyles but if you throw two other really high billionaire in there like Warren Buffett or something then suddenly this extra person would skew the average so far that Divya's and I salaries would melt away and be meaningless and still wouldn't characterize Warren Buffett's salary either. That's why you shouldn't really use averages to characterize this. It strikes fear into people because they think of the million dollar ransoms when 92 percent of averages -- 92 of ransoms are below average. We're working on a paper to describe that.

In this previous paper this is what it looked like in 2020 when we published the paper. We said look the alpha of this power law is a Bellweather. It's a good warning sign, an indicator that things are about to get worse. Sure enough, this is what the landscape looked like a year or so later. And just to be clear, those are on the same scale, which is why I'm flipping back and forth to show you.

Son things did really get worse and it's worth pursuing these metrics and mathematics, because it's not just ivory tour exercise. It matters to be able to predict this stuff because we might change the amount of money that we spend on different defenses and change our approach to law enforcement or policy research according to changes in the ransomware landscape. Another important thing was individual gangs behaved very differently and they demand very different amounts of money. So some of them can charge higher ransoms than others. And, again, that's important if you're hit by a ransomware gaining you might be hit by one of the little ones and not end up -- it might not end up costing you as much. Of course this is just ran some paid instead of losses. But we believe that is also true of losses. The damage functions of different groups are entirely different because the different tooling they use, different structures of their groups and so on. So, again, high correlation coefficient and a p-value that's addressed modeling them as individual gangs does matter. On the left-hand side just repeating and reemphasizing that point, we did a KS distance between all the different ran some distributions for each individual gaining and it shows some sort of differences and similarities between these different groups and the right hand graph we have sort of converted that into the probability, into the p-value that these gainings are the same or different. And so black represents, you know, it's really unlikely these two groups are the same group or that they're attacking the same types of victims and performing in similar way. White usually means it's the same group. And then every color in between is, you know, there's a chance that this group is the same as this other group or behaves in the same way. And that could be a predator effect or could be a prey effect but there is some similarity between the different groups.

So just reiterating you really have to model these groups individually and that's why Divy's approach to the model is crucial. Let's go on to her kind of gamma and beta. My opinion is the frequency of ransomware groups battling over marketshare. So what I mean is, you know, the frequency of it as a whole thing, as a whole phenomenon of ransomware goes up and down based on these different groups appearing, disappearing and battling. It is seasonal and time sensitive. Again, another reason that her modeling is important and she needs access to better data. So the left-hand side here is the number of occurrences per month over 12 month period and the graph on the right is the amount of money by time of

day. So you can see is there is some variation both in times of day, also day of the week, also month of the year. So this stuff really is seasonal and time sensitive but we don't usually talk about it.

>> Divya: I'll give you -- we're at that minute mark.

>> Eireann: One minute to say this is an inverse of the gamma parameter in her model, the proportion of people that paid dead bolt ransoms and the time which they paid them. Over 100 days 8 percent of victims paid and the take away here is, one, most people aren't paying and they still survive but also the people who are paying are paying really quickly. We can use this as a kind of proxy measurement for how people are recovering. And I think I'll say we have some work on the market concentration of ransomware. That will be in our upcoming paper. And if you would like our research and you want to get in touch, please do. Thanks to the DNS Research Federation tore putting me together with another awesome ransomware nerd.

[APPLAUSE]

>> (Away from microphone) as the two speakers were on video we won't be taking questions. I'd like to move without further ado to Mark, our final researcher that we're going to hear from today. We're going to hear about his research. So if you would like to take the podium, Mark, and set up your slides. And then I hope in the -- before 2:30 we can resume our G&A and get your questions and answers but we're also going to go into a break afterwards. So any questions we don't get through because I'm already seeing like loads, week resume the conversation over coffees in the lobby. So Mark, welcome here today and the floor is yours.

>> Mark: Thank you very much. I come from Brazil. I used to do academia in international relations. I moved on to being a NICON counselor nowadays but I try to mix both things. I try to keep both things in sync. In due time I started to arrive at some questions. And I want to share some of those questions with you and hopefully we'll get somewhere together.

(Feedback).

>> All right. So when you look at this title, right, the need for evidence based guidelines to combat health related abuse on the DNS, that's sort of mystical. So let me Boyle this down to something more comprehensible. My question was what is the space of health and what is the intersection between health and Internet governance and I started to arrive very slowly at this interesting phenom Nam which are online pharmacies. Now, you may

have bumped into one. You may use one. They're very practical. In a sense, online pharmacies are very good. They democratize access to mince. They can try different pricing strategies, they can reach different areas, so that's good. But the deeper I dug into them, I started asking this question of, well, but who regulates them? And the more I dug, I found out that the answer is, well, we don't know. Right? It depends. It's a big -- it depends. And that becomestricy, right? When we're talking about mince, we're talking sometimes about over the counter mince, that's fine. Other times we are talking about very restricted very controlled substance that is shouldn't be just sold, right? They need to go to very severe, very specific control. And the problem is when you look at this from a broader perspective, many countries in the world did not have the infrastructure to actually do that control. They cannot exactly account for what kind of mince are being produced and sold within their jurisdiction as well as outside their jurisdiction. So when we look at that in a very simple directed manner, there are a lot of players out there who are selling medicines that should not be sold, sometimes in bulk, sometimes in Quontys that are quite unbelievable and, you know, we're not exactly paying attention to that. It's not an issue that's discussed with Internet governance even though it uses the Internet, it is about policy. It is about, you know, actually harming people using the things we are supposed to take care of, so, you know, that question led me to four years of research, and all of that effort has brought me to ten lines of text I'll represent to you, right? It's a great payoff. So to be able to do that, I have to outline what's the idea here. This is new, right? This is not a preestablished field. It's not drawing from previous experience. It's drawing from the concept that DNS abuse exists, that the infrastructure or the Internet and that the Internet is being abused by actors but it's also acknowledging that we don't have a framework that serves a reference for well what about health related issues? It is seen often as something that's to be regulated by states and within states but the problem is, A, as I explained the states themselves cannot regulate this very well, a lot of them according to the WHO, that's 32 percent of the world's countries that can properly regulate their mince, that leaves 70 percent, and second this is a transnational question. It involves multiple jurisdictions. So how does the state regulate something that's working among many jurisdiction, right? So the idea here is I can and other technical -- right, they do technical standards. I don't know I call this content. I call this more crime but still the thing is around this environment, there's a huge community of people who could be helping alleviate these problems because theres a concept I would like to introduce that stress the notifiers. Some of you have heard of them, some of them have not, but basically these are actors that specialize in dealing with a certain type of crime or occurrence. A lot of that's currently goes towards child sex abuse materials. That's one source that we have. And they were directly with the providers to help take down this material. What would a trusted notifier working with

health related questions look like, and this is the proposal and these are my ten lines of text, right? So eventually going through a lot of literature and a lot of preexisting data, I came to this five points that I would like to socialize with you. This is literally me trying to take this to the community and seeing where we can go with this, right? There are baseline standards that are considered reasonable international standards that we could be following on the Internet and these are minimal standards, right? We could go all the way up and make this super difficult but there are certain things that are simply too basic in the sense that with if we don't -- we are not even following these then what exactly are we doing? Right, like, if we are not following minimal standards or helping minimal standards be followed, aren't we being complicit with something that's clearly harmful illegal and destroying families? Right? So that's the general idea. I'll start with criterion one. So a valid prescription. You would think that's obvious but when you start looking deep into those online pharmacies a lot of them simply don't ask for a prescription at all, never mind legitimate. So what are we doing there, right? Like if this actor is not even asking for the most basic universal thing related to health then it's very likely 99.9 percent an inlegal operation of people trying to basically push, you know, A, medication that is probably not safe, B, even if it's safe, it's unregulated and C there is no accountability for anybody in relation to this. So so second point it's about pharmacists, right? Lot of people don't realize the important of pharmacists in the entire chain, the pharmaceutical chain but when you enter a pharmacy Web site you should be able to consult with one and here's why. Doctors make mistakes? It advertise back to the prescription subject, right? Doctors make mistakes all the time.

>> I'm just going to --

>> Can I help you sir.

>> Just going to adjust the mic a little bit.

>> Perfect. Thank you very much.

>> A quick time check. About two minutes.

>> Perfect.

So in that sense, you need somebody to be that barrier, right? So if your prescription says you need ten boxes of Fentanyl, that's probably wrong. It's probably one, right? So that's the sort of basic, very basic standard that we are not observing, right? Criterion three is where is that pharmacy actually based? Hey, it's own line, the Internet is global but that's kind of the center of the problem. There are many divergent standards. Certain countries

are known to have very loose laws and if we cannot even understand where they're from we cannot advise people, we cannot create engagement and tell them if it is from this place you're probably not being protected by anything, right? There is actually no regulation protecting you in any way, shape, or form. So just to go real quick, No. 4, they need to be approved by the national regulatory agency of the country and finally, criterion five and that's the big issue, right? There are certain categories of medication that we know should be controlled and this is a global consensus. And yet on the Internet we are somehow letting that slip. We're like oh, okay, you want to buy tons of cases of antibiotics, here. Right, that sort of gap is something that to a lot of research and going to this Web site over and over again, it's very lucrative, we are doing absolutely nothing to stop it. We are leaving it mostly to Interpol right now. It's great that they're doing something but at the same time it is the space that we are supposed to be stewards of. So how do we kick start at least with these minimal requirements something that we start looking to introduce and this has a bit of a spill over effect? How do we get, you know, some registrars on board to start looking into these matters because right now talking to the different registrars and registries, when they receive complaints of things like this it goes into this general abuse pile. Now, I'm not saying credit card fraud is not bad. It's bad. But this is a little bit worse. This is actual lives that we are talking about. This is a different kind of category. So my idea has been to try to introduce this and luckily some actors have been listening and with the great help -- without your help, this wouldn't be happening at all because at first it was like oh this is not even an issue. This is content. Yeah, it is content but how much can we distance ourselves from something that's actually a responsibility to help people not be harmed by these criminals? So I will wrap that up with leaving my contacts and I'll be discussing this more during ICANN and during upcoming meetings at the IGF and so on. But this is a conversation starter, right? I'm not trying to really tell anyone that this is the way it should be. I'm just introducing a topic that hopefully we can discuss as a community. Thank you very much for your time. Thank you everyone.

[APPLAUSE]

>> Moderator: Thank you very much, Mark, for that very high level view of an outstanding piece of work. So I know that there were several people I didn't even get to this side of the room and there's two people here waiting to answer -- ask questions. Who would like to make an intervention? Just raise your hand. Okay, lots and lots of people.

>> (Away from microphone).

>> There's Kanye, Angela, a lady there. There's a whole batch here. Almost everybody in the room. So I'm going to take groups of three and we'll just get through as many as we can in the last ten minutes, okay?

Go.

[LAUGHTER]

>> Show time.

>> No pressure, Buddy.

>> So for Derrick, with the UDRP, even as trademark holders file UDRPs, still expensive and a cumbersome process. So I'm wondering if you guys in your research are spotting any gaps, you know, that the UDRP process is -- there may be hurdles which there are things which maybe can be improved. So that's No. 1. And for Mark my question is in working with public safety agencies like the FDA and DEA here in the U.S., they've had real problems with registrars or registries, some of them have signed the trusted notifiers but they really haven't taken down these counterfeit, you know, sites that offer counterfeit drugs or even illegal drugs. So I was just wondering how your paper might address that?

>> I think there -- we'll take yours first and then come back. We'll go over -- sweep up this side of the room next.

>> Thank you. So I was just curious to know whether there is a repeal process within the UDRP for example of a decision that has already been taken. If so, how long that process takes and if there is any example of such? Thanks.

>> I just wanted to get a little bit of understanding of how UDRP structure in legal justice system and if a decision is made by UDRP can it be challenged and if it is challenged how would that compare with a foreign country.

So all I was trying to say how does this compare with the American legal justice system and if one goes out and files a lawsuit in courts here and the other parties in a different country how would they respond to it and if he don't have the means to hire an attorney here how would they respond to it in that case.

>> Moderator: Quite a lot of UDP questions, guys.

Is there an appeals system, how does it relate to the justice system, can it be challenged in court and did you identify any gaps in your research that you would like to see the UDRP addressing and for Mark, there was a question about, you know, the headway that you're

making in the public safety community. You talked about registry and registrar engagement. So we'll come back. So let's do UDRP and then drugs.

>> Derrick: All right. I'll take a quick pass and then see if Andrew and Haiman have any additional comments.

First with bobby's question. I think there's still work to go to identify any potential gaps. I think the good news for trademark holders is they win. And so it is a relatively fast process. The more delay you have, the more it hurts trademark holders because the more a potential -- let's use the term cyber squader can benefit from the domain that they've registered. So it's generally a trademark friendly fast process that is relatively inexpensive if you compare it to extensive liptgation and so forth. That's a -- that's good news, I think. But we'll keep looking to see are there other gaps to consider for both trademark holders and some of these grair areas where it's not so clear that it should be confiscated from a previous registrant. In terms of the appeal process, so within the UDRP there is no appeal process and that's been one of the concerns. There are a lot of recommendations for reform of this process and other people say it doesn't need reform. It's working relatively well. Coming to your question in a second. And so if you look at some of the things that could be possibly appealed -- reformed, one suggestion is to not let the complainant choose to which the RSP it submits, that they could submit the complaint to ICANN and ICANN could randomly like the courts do and so forth, assign it to a particular DRSP. That's a possible reform another reform, proposal that I don't like is that this process not be so public. There are proposals to not have the results public and not publish the data that we love and crave. So I don't like that proposal. In terms of the legal understanding and my understanding and Emily and others can correct me if I'm wrong, so once you go to this process, although there's no appeal within ICANN, I believe you could resort to a legal structure. But then you run the problems that you already are alluding to which legal structure would have jurisdiction, how would you deal with so many of the complexities and expense that would come from that and that's why this is seen as such a valuable process and has lasted for 23 years because it is serving the purpose that -- for which it was created.

Anybody else want to --

>> Moderator: I want to just come to Mark on the engagement with public safety but yes, you're right, there's a moratorium that could be the end of the process to allow for legal challenge in court. So it doesn't sort of block a legal challenge in court.

Mark, your engagement with the public (Away from microphone).

>> Mark: Thank you. So that question is perfect because the federal administration of the U.S. has engaged in a pilot to stop opioids together with three major providers of the DNS space. However, it was a very isolated project. That's the thing that left me questioning the efficacy of you doing something very targeted and very specific with a limited set of players we are trying to engage a broader academic community, the -- because it ended up existing in its own bubble. So there is awareness of the issue at some level but the question is how do you bring this to the notice of the community in a way that we can actually get something started in a broader sense but we do have that ledge massy of having a major body already carrying out that sort of research that gives us the safety that, okay, this is an issue, it is actionable but how do we bring this now to the next level? I think that's the real question and the thing we need to start looking moving forward.

Thank you.

>> Moderator: Andrew, you wanted to say a couple of words.

>> Yeah, and one more thing about the change in structure is -- yeah, so we have seen a few papers that said that, because you can do one panel, three panel and we've seen that three panels respondents tend to win at a more fair rate. So in addition to the randomsation, I think just standardizing and having three panelists will just make things easier. That way it can be, you know, yes, yes, no.

>> Moderator: Thank you. I know we've got -- we're out of time. I think I'm going to be kind to you because we've eaten into the breaks every time. And I think we've all worked really hard and need a break. So what I suggest is those of you and who I'm sorry I didn't get to your questions, Angela, Kanye, the ladies there, please, please let's grab some refreshment out in the lobby. Please come and talk to the panel. And please can I also just -- and in Room 603 there is a fantastic demonstration of the DAP platform. And there are many researchers in the room. Please do come and have a look at that. And talk to the team because we love working with researchers and are always looking for more engagement from the research community. So can I ask you to thank our wonderful panel for their incredible insights today.

[APPLAUSE]